UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
-v-	:	DECLARATION OF STEVEN M. BELLOVIN, Ph.D., IN SUPPORT OF SUPPRESSION
JOSHUA ADAM SCHULTE,	:	17 Cr. 548 (PAC)
Defendant.	:	

STEVEN M. BELLOVIN, Ph.D., declares under penalty of perjury:

1. I am the Percy K. and Vida L.W. Hudson Professor of Computer Science at Columbia University, where I have taught since 2005. I make this declaration for the limited purpose of providing expert support for Defendant Joshua Adam Schulte's motion to suppress and for an evidentiary hearing under *Franks v. Delaware*, 438 U.S. 154 (1978). This declaration is based on my personal knowledge (including my training and experience as a computer scientist), my review of documents produced by the government in discovery, and my discussions with members of Mr. Schulte's defense team.

2. Because this declaration is being made for a limited purpose, it does not include everything I know about this case or the matters discussed herein.

My Qualifications

3. My curriculum vitae is annexed hereto as Exhibit "A." In summary, I received my doctorate in computer science in 1982 from the University of North Carolina at Chapel Hill. I am currently the Percy K. and Vida L.W. Hudson Professor of Computer Science at Columbia University and an affiliate faculty member at Columbia Law School. I have been a Professor of Computer Science at Columbia since 2005. I have also worked as Chief

Technologist for the Federal Trade Commission (2012–2013), Adjunct Professor of Computer Science at the University of Pennsylvania (2002–2004), and as a consultant and research fellow for AT&T (1998–2012).

4. I am also a member of the National Academy of Engineering ("National Academy") and have served on many National Academy study committees and the National Academy's Computer Science and Telecommunications Board. I have also been part of the leadership of the Internet Engineering Task Force, serving on the Internet Architecture Board and as a Security Area Director. I have also served on several advisory committees at the Department of Homeland Security and the Election Assistance Commission.

5. I have published extensively on a wide range of subjects relating to Internet security, computer science, and forensic computer analysis.

The Meaning and Significance of a Computer's "Page File"

6. I understand that when the government applied in April 2017 for a warrant to search Mr. Schulte's devices for evidence of child pornography, the government claimed it had found a single "photograph" or image of what "appear[ed] to be child pornography" on Mr. Schulte's "desktop computer."

7. In fact, according to documents produced by the government in discovery, the image was discovered in a specific area of Mr. Schulte's desktop computer known as the "page file." This location should have been obvious to the investigating agents because the "file path" of the image—the written description of where on the computer the image was found—indicates that it was found within "pagefile.sys," an unmistakable reference to the page file.

8. A "page file" (sometimes referred to as a "paging file" or "swap file") is an area of the computer that acts as an extension of the computer's Random Access Memory (RAM). If information in RAM is not actively being used by the computer, or has not recently been used, the operating system (e.g., Windows) may move it to the page file in order to free up memory space in RAM.

9. Significantly, the operating system, not the computer's user, creates and maintains the page file. Indeed, the contents of the page file are generally not accessible to the computer's user. Similarly, computer users generally cannot modify or determine the contents of a page file. And the contents of a page file do not have file names and do not resemble ordinary user files.

10. Because of the nature of a page file, the presence of a photograph or other image in a page file, standing alone, does not provide a basis for concluding that the photograph or image was ever knowingly accessed, received, possessed, or even seen by a computer user. For example, when a computer user visits an Internet website, the web browser can automatically "pre-fetch" or download images into RAM from the website, thus allowing them to be stored in the page file, even if the user never viewed those images or intentionally "clicked" on them. An image can thus end up in the computer's page file without the user's knowledge—and even if the user never saw it, intentionally accessed it, or knowingly acquired it. Indeed, since the page file contains pieces of RAM that have not been used recently, the presence of an image on the page file is suggestive of an image that was not viewed recently, if at all.

11. In this case, moreover, the limited "metadata" associated with the image—the information about the origin or format of the image—does not indicate when the image was

created, accessed, or last viewed by a user (if ever). Accordingly, the image may have been residing in the page file of Mr. Schulte's computer for a long period of time before it was discovered by law enforcement—indeed, it may have been there ever since the computer was first used. Put another way, the mere fact that the image was found in Mr. Schulte's page file in April 2017 does not show that it had arrived on the computer recently, as opposed to many months or years earlier.

12. Finally, about 20 percent of the image is blacked out. While there are various reasons this may have occurred, the blacking out is consistent with the image having been automatically downloaded to Mr. Schulte's computer, and stored to the page file, without him ever seeing or knowingly acquiring it.

I declare under penalty of perjury that the foregoing is true and correct.

Dated: New York, New York
June 28, 2019

Steven M. Bellovin, Ph.D.

Exhibit A

Steven M. Bellovin

Percy K. and Vida L.W. Professor of Computer Science

smb at cs.columbia.edu
http://www.cs.columbia.edu/~ smb

Education

1982 Ph.D., University of North Carolina at Chapel Hill. Dissertation: *Verifiably Correct Code Generation Using Predicate Transformers*; advisor: David L. Parnas.

1977 M.S., University of North Carolina at Chapel Hill.

1972 B.A., Columbia University.

Employment

2014–now Percy K. and Vida L.W. Professor of Computer Science, Columbia University.

2005–2014 Professor of Computer Science, Columbia University.

2012–2013 Chief Technologist, Federal Trade Commission

2002–2004 Adjunct Professor of Computer Science, University of Pennsylvania.

2005–2012 AT&T, consultant

1998–2004 AT&T Fellow, AT&T Labs—Research.

1987–1998 Distinguished Member of the Technical Staff, AT&T Bell Laboratories and AT&T Labs—Research.

1982–1987 Member of the Technical Staff, AT&T Bell Laboratories.

1977–1978 Instructor, Dept. of Computer Science, University of North Carolina at Chapel Hill.

Honors

2014 Elected to the Cybersecurity Hall of Fame

2006 Received the 2007 NIST/NSA National Computer Systems Security Award

2001 Elected to the National Academy of Engineering.

1998 Named an AT&T Fellow.

1995 Received the Usenix Lifetime Achievement Award ("The Flame"), along with Tom Truscott and Jim Ellis, for our role in creating Usenet.

Books and Chapters

- Salvatore Stolfo, Steven M. Bellovin, Angelos D. Keromytis, Sara Sinclair, Sean Smith, and Shlomo Hershkop, editors. *Insider Attack and Cyber Security: Beyond the Hacker (Advances in Information Security)*. Springer, 2008.
- Seymour E. Goodman and Herbert S. Lin, editors. *Toward a Safer and More Secure Cyberspace*. National Academy Press, 2007.
- Stephen T. Kent and Lynette I. Millett, editors. *Who Goes There? Authentication Through the Lens of Privacy*. National Academies Press, 2003.
- John L. Hennessy, David A. Patterson, and Herbert S. Lin, editors. *Information Technology for Counterterrorism: Immediate Actions and Future Possibilities*. National Academies Press, 2003.
- William R. Cheswick, Steven M. Bellovin, and Aviel D. Rubin. *Firewalls and Internet Security; Repelling the Wily Hacker*. Addison-Wesley, Reading, MA, second edition, 2003.
- *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. National Academies Press, 2002.
- Stephen T. Kent and Lynette I. Millett, editors. *IDs—Not That Easy: Questions About Nationwide Identity Systems*. National Academies Press, 2002.
- Fred B. Schneider, editor. *Trust in Cyberspace*. National Academy Press, 1999.
- Network security issues. In Peter Denning and Dorothy Denning, editors, *Internet Besieged: Countering Cyberspace Scofflaws*. ACM Press, 1997.
- Network security issues. In A. Tucker, editor, *CRC Computer Science and Engineering Handbook*. CRC Press, 1996.
- Security and software engineering. In B. Krishnamurthy, editor, *Practical Reusable UNIX Software*. John Wiley & Sons, 1995.
- William R. Cheswick and Steven M. Bellovin. *Firewalls and Internet Security: Repelling the Wily Hacker*. Addison-Wesley, Reading, MA, first edition, 1994.

Papers and Articles

- Steven M. Bellovin, Matt Blaze, and Susan Landau. Comments on proposed remote search rules, October 2014.
- Steven M. Bellovin. The economics of cyberwar. Technical Report CUCS-010-14, Department of Computer Science, Columbia University, April 2014. Presented at the Institute for New Economic Thinking's *Human After All*.

- Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau. Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet. *Northwestern Journal of Technology & Intellectual Property*, 12(1), 2014.
- Steven M. Bellovin, Renée M. Hutchins, Tony Jebara, and Sebastian Zimmeck. When enough is enough: Location tracking, mosaic theory, and machine learning. *NYU Journal of Law and Liberty*, 8(2):555–628, 2014.
- Sebastian Zimmeck and Steven M. Bellovin. Privee: An architecture for automatically analyzing web privacy policies. In *23rd USENIX Security Symposium (USENIX Security 14)*, pages 1–16, San Diego, CA, August 2014. USENIX Association.
- Steven M. Bellovin. Position paper: Security and simplicity. In *W3C/IAB Workshop on Strengthening the Internet Against Pervasive Monitoring (STRINT)*, March 2014.
- Binh Vo and Steven Bellovin. Anonymous publish-subscribe systems. In *SECURECOMM*, Beijing, September 2014.
- Vasilis Pappas, Fernando Krell, Binh Vo, Vlad Kolesnimov, Tal Malkin, Seung Geol Choi, Wesley George, Angelos Keromytis, and Steven M. Bellovin. Blind seer: A scalable private DBMS. In *IEEE Symposium on Security and Privacy*, May 2014.
- Steven M. Bellovin. Mysterious checks from Mauborgne to Fabyan. Technical Report CUCS-012-14, Department of Computer Science, Columbia University, April 2014. A later version will appear in *Cryptologia*.
- Steven M. Bellovin. Vernam, Mauborgne, and Friedman: The one-time pad and the index of coincidence. Technical Report CUCS-014-14, Department of Computer Science, Columbia University, May 2014.
- S. Bellovin, R. Bush, and D. Ward. Security Requirements for BGP Path Validation. RFC 7353, RFC Editor, August 2014.
- Steven M. Bellovin. What should crypto look like? *IEEE Security & Privacy*, 12(6):108–108, November 2014.
- Steven M Bellovin. Dr. Strangecode. *IEEE Security & Privacy*, 12(3), May–June 2014.
- Steven M. Bellovin. Submission to the Privacy and Civil Liberties Oversight Board: Technical issues raised by the Section 215 and Section 702 surveillance programs, July 2013.
- Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau. Going bright: Wiretapping without weakening communications infrastructure. *IEEE Security & Privacy*, 11(1):62–72, January–February 2013.

- Steven M. Bellovin. Why healthcare.gov has so many problems. *CNN.com*, October 15 2013.
- Steven M. Bellovin. Military cybersomethings. *IEEE Security & Privacy*, 11(3):88, May–June 2013.
- Steven M. Bellovin. Walls and gates. *IEEE Security & Privacy*, 6(11), November-December 2013.
- Steven M. Bellovin, Scott O. Bradner, Whitfield Diffie, Susan Landau, and Jennifer Rexford. Can it really work? Problems with extending EINSTEIN 3 to critical infrastructure. *National Security Journal*, 3, 2012.
- Carl Landwehr, Dan Boneh, John Mitchell, Steven M. Bellovin, Susan Landau, and Mike Lesk. Privacy and cybersecurity: The next 100 years. *Proceedings of the IEEE*, PP(99):1–15, 2012.
- Maritza Johnson, Serge Egelman, and Steven M. Bellovin. Facebook and privacy: It's complicated. In *Symposium On Usable Privacy and Security (SOUPS)*, July 2012.
- Michelle Madejski, Maritza Johnson, and Steven M. Bellovin. A study of privacy setting errors in an online social network. In *Proceedings of SESOC 2012*, 2012.
- Mariana Raykova, Hang Zhao, and Steven M. Bellovin. Privacy enhanced access control for outsourced data sharing. In *Financial Cryptography and Data Security*, March 2012.
- Mariana Raykova, Ang Cui, Binh Vo, Bin Liu, Tal Malkin, Steven M. Bellovin, and Salvatore J. Stolfo. Usable secure private search. *IEEE Security & Privacy*, 10(5), September-October 2012.
- F. Gont and S. Bellovin. Defending against Sequence Number Attacks. RFC 6528, RFC Editor, February 2012.
- Steven M. Bellovin. The major cyberincident investigations board. *IEEE Security & Privacy*, 10(6):96, November–December 2012.
- Steven M. Bellovin. Fighting the last war. *IEEE Security & Privacy*, 10(3), May–June 2012.
- Steven M. Bellovin, Scott O. Bradner, Whitfield Diffie, Susan Landau, and Jennifer Rexford. As simple as possible—but not more so. *Communications of the ACM*, 2011. Note: this is a shorter version of "Can it really work?".
- Maritza L. Johnson, Steven M. Bellovin, and Angelos D. Keromytis. Computer security research with human subjects: Risks, benefits and informed consent. In *Financial Cryptography and Data Security*, Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 2011.

- Michelle Madejski, Maritza Johnson, and Steven M. Bellovin. The failure of online social network privacy settings. Technical Report CUCS-010-11, Department of Computer Science, Columbia University, February 2011.
- Sal Stolfo, Steven M. Bellovin, and David Evans. Measuring security. *IEEE Security & Privacy*, 9(3):88, May–June 2011.
- Hang Zhao, Jorge Lobo, Arnab Roy, and Steven M Bellovin. Policy refinement of network services for MANETs. In *The 12th IFIP/IEEE International Symposium on Integrated Network Management (IM 2011)*, Dublin, Ireland, May 2011.
- Steven M. Bellovin. Frank Miller: Inventor of the one-time pad. Technical Report CUCS-009-11, Department of Computer Science, Columbia University, March 2011. A revised version appeared in *Cryptologia* 35(3), July 2011.
- Mariana Raykova, Hang Zhao, and Steven M. Bellovin. Privacy enhanced access control for outsourced data sharing. Technical Report CUCS-039-11, Department of Computer Science, Columbia University, 2011.
- Vasilis Pappas, Mariana Raykova, Binh Vo, Steven M. Bellovin, and Tal Malkin. Private search in the real world. In *Proceedings of the 2011 Annual Computer Security Applications Conference*, December 2011.
- Steven M. Bellovin. Clouds from both sides. *IEEE Security & Privacy*, 9(3), May–June 2011.
- Steven M. Bellovin. Security think. *IEEE Security & Privacy*, 9(6), November–December 2011.
- Maritza Johnson and Steven M. Bellovin. Policy management for e-health records. Usenix HealthSec, August 2010. Position paper.
- Hang Zhao and Steven M. Bellovin. High performance firewalls in MANETs. In *International Conference on Mobile Ad-hoc and Sensor Networks*, pages 154–160, December 2010.
- Shreyas Srivatsan, Maritza Johnson, and Steven M. Bellovin. Simple-VPN: Simple IPsec configuration. Technical Report CUCS-020-10, Department of Computer Science, Columbia University, July 2010.
- Elli Androulaki, Binh Vo, and Steven M. Bellovin. A real-world identity management system with master secret revocation. Technical Report CUCS-008-10, Department of Computer Science, Columbia University, April 2010.
- Elli Androulaki and Steven M. Bellovin. A secure and privacy-preserving targeted ad-system. In *Proceedings of the 1st Workshop on Real-Life Cryptographic Protocols and Standardization*, January 2010.

- Vasilis Pappas, Mariana Raykova, Binh Vo, Steven M. Bellovin, and Tal Malkin. Trade-offs in private search. Technical Report CUCS-022-10, Department of Computer Science, Columbia University, September 2010.
- Elli Androulaki, Binh Vo, and Steven M. Bellovin. Privacy-preserving, taxable bank accounts. In *Proceedings of the European Symposium on Research in Computer Security (ESORICS)*, Athens, September 2010. Longer version issued as Tech Report CUCS-005-10.
- Elli Androulaki, Binh Vo, and Steven M. Bellovin. Privacy-preserving, taxable bank accounts. Technical Report CUCS-005-10, Department of Computer Science, Columbia University, April 2010.
- Steven M. Bellovin. Identity and security. *IEEE Security & Privacy*, 8(2), March–April 2010.
- Steven M. Bellovin. Perceptions and reality. *IEEE Security & Privacy*, 8(5), September–October 2010.
- Elli Androulaki, Binh Vo, and Steven M. Bellovin. Cybersecurity through identity management. In *Engaging Data: First International Forum on the Application and Management of Personal Electronic Information*, October 2009.
- Steven M. Bellovin and Randy Bush. Configuration management and security. *IEEE Journal on Selected Areas in Communications*, 27(3):268–274, April 2009.
- Shaya Potter, Steven M. Bellovin, and Jason Nieh. Two person control administration: Preventing administration faults through duplication. In *LISA '09*, November 2009.
- Maritza Johnson, Steven M. Bellovin, Robert W. Reeder, and Stuart Schechter. Laissez-faire file sharing: Access control designed for individuals at the endpoints. In *New Security Paradigms Workshop*, September 2009.
- Hang Zhao and Steven M. Bellovin. Source prefix filtering in ROFL. Technical Report CUCS-033-09, Department of Computer Science, Columbia University, July 2009.
- Yuu-Heng Cheng, Mariana Raykova, Alex Poylisher, Scott Alexander, Martin Eiger, and Steve M. Bellovin. The Zodiac policy subsystem: a policy-based management system for a high-security MANET. In *IEEE Policy 2009*, July 2009. Longer version issued as CUCS-023-09.
- Yuu-Heng Cheng, Scott Alexander, Alex Poylisher, and Mariana Raykova Steven M. Bellovin. The Zodiac policy subsystem: a policy-based management system for a high-security MANET. Technical Report CUCS-023-09, Department of Computer Science, Columbia University, May 2009.

- Elli Androulaki and Steven M. Bellovin. An anonymous credit card system. In *Proceedings of 6th International Conference on Trust, Privacy & Security in Digital Business (TrustBus)*, September 2009. Longer version issued as Tech Report CUCS-010-09.
- Elli Androulaki and Steven M. Bellovin. An anonymous credit card system. Technical Report CUCS-010-09, Department of Computer Science, Columbia University, February 2009.
- Elli Androulaki and Steven M. Bellovin. Anonymous delivery of physical objects. In *Symposium on Privacy-Enhancing Technologies (PET)*, July 2009.
- Elli Androulaki and Steven M. Bellovin. A secure and privacy-preserving targeted ad-system. Technical Report CUCS-044-09, Department of Computer Science, Columbia University, October 2009. A revised version will appear at the 1st Workshop on Real-Life Cryptographic Protocols and Standardization.
- Mariana Raykova, Binh Vo, Tal Malkin, and Steven M. Bellovin. Secure anonymous database search. In *Proceedings of the ACM Cloud Computing Security Workshop*, November 2009.
- S. Bellovin. Guidelines for Specifying the Use of IPsec Version 2. RFC 5406, RFC Editor, February 2009.
- Steven M. Bellovin. The government and cybersecurity. *IEEE Security & Privacy*, 7(2), March–April 2009. (Ignore the part that says I work for Microsoft—I don't. . . The editor and I both missed that in the galleys.).
- Steven M. Bellovin. Security as a systems property. *IEEE Security & Privacy*, 7(5), September–October 2009.
- Maritza Johnson, Chaitanya Atreya, Adam Aviv, Mariana Raykova, Steven M. Bellovin, and Gail Kaiser. RUST: The reusable security toolkit, 2008. Draft.
- Steven M. Bellovin, Matt Blaze, Whitfield Diffie, Susan Landau, Peter G. Neumann, and Jennifer Rexford. Risking communications security: Potential hazards of the "Protect America Act". *IEEE Security & Privacy*, 6(1):24–33, January–February 2008.
- Kyle Dent and Steven M. Bellovin. Newspeak: A secure approach for designing web applications. Technical Report CUCS-008-08, Department of Computer Science, Columbia University, February 2008.
- Hang Zhao, Jorge Lobo, and Steven M. Bellovin. An algebra for integration and analysis of Ponder2 policies. In *Proceeding of the 9th IEEE Workshop on Policies for Distributed Systems and Networks*, June 2008.
- Hang Zhao, Chi-Kin Chau, and Steven M. Bellovin. ROFL: Routing as the firewall layer. In *New Security Paradigms Workshop*, September 2008. A version is available as Technical Report CUCS-026-08.

- Maritza Johnson, Chaitanya Atreya, Adam Aviv, Mariana Raykova, Steven M. Bellovin, and Gail Kaiser. RUST: A retargetable usability testbed for website authentication technologies. In *Usenix Workshop on Usability, Psychology, and Security*, April 2008.
- Maritza Johnson and Steven M. Bellovin. Security assurance for web device APIs. In *Security for Access to Device APIs from the Web - W3C Workshop*, December 2008.
- Elli Androulaki, Mariana Raykova, Angelos Stavrou, and Steven M. Bellovin. PAR: Payment for anonymous routing. In *Proceedings of the 8th Privacy Enhancing Technologies Symposium*, July 2008.
- Elli Androulaki, Seung Geol Choi, Steven M. Bellovin, and Tal Malkin. Reputation systems for anonymous networks. In *Proceedings of the 8th Privacy Enhancing Technologies Symposium*, July 2008.
- Olaf Maennel, Randy Bush, Luca Cittadini, and Steven M. Bellovin. A better approach than carrier-grade-NAT. Technical Report CUCS-041-08, Department of Computer Science, Columbia University, September 2008.
- Steven M. Bellovin. Security by checklist. *IEEE Security & Privacy*, 6(2), March–April 2008.
- Steven M. Bellovin. The puzzle of privacy. *IEEE Security & Privacy*, 6(5), September–October 2008.
- Steven M. Bellovin, Matt Blaze, Whitfield Diffie, Susan Landau, Peter G. Neumann, and Jennifer Rexford. Internal surveillance, external risks. *Communications of the ACM*, 50(12), December 2007.
- Hang Zhao and Steven M. Bellovin. Policy algebras for hybrid firewalls. Technical Report CUCS-017-07, Department of Computer Science, Columbia University, March 2007. Also presented at the Annual Conference of the ITA, 2007.
- Sotiris Ioannidis, Steven M. Bellovin, John Ioannidis, Angelos D. Keromytis, Kostas Anagnostakis, and Jonathan M. Smith. Coordinated policy enforcement for distributed applications. *International Journal of Network Security*, 4(1):69–80, January 2007.
- Steven M. Bellovin and William R. Cheswick. Privacy-enhanced searches using encrypted Bloom filters. Technical Report CUCS-034-07, Department of Computer Science, Columbia University, September 2007.
- Elli Androulaki, Mariana Raykova, Angelos Stavrou, and Steven M. Bellovin. Opentor: Anonymity as a commodity service. Technical Report CUCS-031-07, Department of Computer Science, Columbia University, September 2007.
- Elli Androulaki, Seung Geol Choi, Steven M. Bellovin, and Tal Malkin. Reputation systems for anonymous networks. Technical Report CUCS-029-07, Department of Computer Science, Columbia University, September 2007.

- S. Bellovin. Key Change Strategies for TCP-MD5. RFC 4808, RFC Editor, March 2007.
- Steven M. Bellovin. DRM, complexity, and correctness. *IEEE Security & Privacy*, 5(1), January–February 2007.
- Steven M. Bellovin. Seers and craftspeople. *IEEE Security & Privacy*, 5(5), September–October 2007.
- Paula Hawthorn, Barbara Simons, Chris Clifton, David Wagner, Steven M. Bellovin, Rebecca Wright, Arnold Rosenthal, Ralph Poore, Lillie Coney, Robert Gellman, and Harry Hochheiser. Statewide databases of registered voters: Study of accuracy, privacy, usability, security, and reliability issues, February 2006. Report commissioned by the U.S. Public Policy Committee of the Association for Computing Machinery.
- Steven M. Bellovin, Matt Blaze, Ernest Brickell, Clinton Brooks, Vint Cerf, Whitfield Diffie, Susan Landau, Jon Peterson, and John Treichler. Security implications of applying the Communications Assistance to Law Enforcement Act to Voice over IP, 2006.
- Steven M. Bellovin, David D. Clark, Adrian Perrig, and Dawn Song. Workshop report: Clean-slate design for the next-generation secure Internet, March 2006. NSF workshop report.
- Ka-Ping Yee, David Wagner, Marti Hearst, and Steven M. Bellovin. Prerendered user interfaces for higher-assurance electronic voting. In *Usenix/ACCURATE Electronic Voting Technology Workshop*, August 2006. An earlier version appeared as Technical Report UCB/EECS-2006-35.
- Steven M. Bellovin, Angelos Keromytis, and Bill Cheswick. Worm propagation strategies in an IPv6 Internet. *;login:*, pages 70–76, February 2006.
- Steven M. Bellovin. Virtual machines, virtual security. *Communications of the ACM*, 49(10), October 2006. "Inside RISKS" column.
- Steven M. Bellovin and Eric K. Rescorla. Deploying a new hash algorithm. In *Proceedings of NDSS '06*, 2006.
- S. Bellovin and A. Zinin. Standards Maturity Variance Regarding the TCP MD5 Signature Option (RFC 2385) and the BGP-4 Specification. RFC 4278, RFC Editor, January 2006.
- Steven M. Bellovin. Unconventional wisdom. *IEEE Security & Privacy*, 4(1), January–February 2006.
- Steven M. Bellovin. On the brittleness of software and the infeasibility of security metrics. *IEEE Security & Privacy*, 4(4), July–August 2006.

- Steven M. Bellovin, Matt Blaze, and Susan Landau. The real national-security needs for VoIP. *Communications of the ACM*, 48(11), November 2005. "Inside RISKS" column.
- S. Bellovin and R. Housley. Guidelines for Cryptographic Key Management. RFC 4107, RFC Editor, June 2005.
- Steven M. Bellovin. Security and privacy: Enemies or allies? *IEEE Security & Privacy*, 3(3), May–June 2005.
- Steven M. Bellovin. A look back at "Security problems in the TCP/IP protocol suite". In *Annual Computer Security Applications Conference*, December 2004. Invited paper.
- William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, and Omer Reingold. Just fast keying: Key agreement in a hostile Internet. *ACM Transactions on Information and System Security (TISSEC)*, 7(2):1–32, May 2004.
- Steven M. Bellovin. Spamming, phishing, authentication, and privacy. *Communications of the ACM*, 47(12), December 2004. "Inside RISKS" column.
- Steven M. Bellovin. Cybersecurity research needs, July 2003. Testimony before the House Select Committee on Homeland Security, Subcommittee on Cybersecurity, Science, Research, & Development, hearing on "Cybersecurity—Getting it Right".
- Steven M. Bellovin. Access control prefix router advertisement option for IPv6. Obsolete Internet draft, February 2003.
- Steven M. Bellovin, Marcus Leech, and Tom Taylor. ICMP traceback messages. Obsolete Internet draft, February 2003.
- Steven M. Bellovin and Emden R. Gansner. Using link cuts to attack Internet routing, 2003. Draft.
- Sotiris Ioannidis, Steven M. Bellovin, John Ioannidis, Angelos D. Keromytis, and Jonathan M. Smith. Design and implementation of virtual private services. In *Proceedings of the IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Workshop on Enterprise Security*, Linz, Austria, June 2003.
- S. Bellovin. The Security Flag in the IPv4 Header. RFC 3514, RFC Editor, April 1, 2003.
- S. Bellovin, J. Ioannidis, A. Keromytis, and R. Stewart. On the Use of Stream Control Transmission Protocol (SCTP) with IPsec. RFC 3554, RFC Editor, July 2003.
- Steven M. Bellovin and Randy Bush. Security through obscurity considered dangerous. Obsolete Internet draft, February 2002.

- Ratul Mahajan, Steven M. Bellovin, Sally Floyd, John Ioannidis, Vern Paxson, and Scott Shenker. Controlling high bandwidth aggregates in the network. *Computer Communication Review*, 32(3):62–73, July 2002.
- John Ioannidis and Steven M. Bellovin. Implementing pushback: Router-based defense against DDoS attacks. In *Proc. Internet Society Symposium on Network and Distributed System Security*, 2002.
- Sotiris Ioannidis, Steven M. Bellovin, and Jonathan Smith. Sub-operating systems: A new approach to application security. In *SIGOPS European Workshop*, September 2002.
- William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, and Omer Reingold. Efficient, DoS-resistant, secure key exchange for internet protocols. In *Proceedings of the ACM Computer and Communications Security (CCS) Conference*, November 2002.
- Steven M. Bellovin. A technique for counting NATted hosts. In *Proc. Second Internet Measurement Workshop*, pages 267–272, Marseille, 2002.
- Steven M. Bellovin. A "Reason" field for ICMP "Administratively Prohibited" messages. Obsolete Internet draft, December 2001.
- Steven M. Bellovin. Using Bloom Filters for authenticated yes/no answers in the DNS. Obsolete Internet draft, December 2001.
- Steven M. Bellovin. Computer security—an end state? *Communications of the ACM*, 44(3), March 2001.
- Sotiris Ioannidis and Steven M. Bellovin. Building a secure web browser. In *Usenix Conference*, June 2001.
- Peter M. Gleitz and Steven M. Bellovin. Transient addressing for related processes: Improved firewalling by using IPv6 and multiple addresses per host. In *Proceedings of the Eleventh Usenix Security Symposium,*, August 2001.
- S.M. Bellovin and M.A. Blaze. Cryptographic modes of operation for the Internet. In *Second NIST Workshop on Modes of Operation*, August 2001.
- Steven M. Bellovin, C. Cohen, J. Havrilla, S. Herman, B. King, J. Lanza, L. Pesante, R. Pethia, S. McAllister, G. Henault, R. T. Goodden, A. P. Peterson, S. Finnegan, K. Katano, R. M. Smith, and R. A. Lowenthal. Results of the "Security in ActiveX Workshop", December 2000.
- D. Whiting, B. Schneier, and S. Bellovin. AES key agility issues in high-speed IPsec implementations, 2000.
- Steven M. Bellovin, Matt Blaze, David Farber, Peter Neumann, and Gene Spafford. Comments on the Carnivore system technical review draft, December 2000.

- Steven M. Bellovin and Robert G. Moskowitz. Client certificate and key retrieval for IKE. Obsolete Internet draft, November 2000.
- Matt Blaze and Steven M. Bellovin. Open Internet wiretapping, July 2000. Written testimony for a hearing on "Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program" by the Subcommittee on the Constitution, House Judiciary Committee.
- Matt Blaze and Steven M. Bellovin. Tapping on my network door. *Communications of the ACM*, 43(10), October 2000.
- Steven M. Bellovin. Wiretapping the Net. *The Bridge*, 20(2):21–26, Summer 2000.
- Sotiris Ioannidis, Angelos D. Keromytis, Steven M. Bellovin, and Jonathan M. Smith. Implementing a distributed firewall. In *ACM Conference on Computer and Communications Security*, Athens, Greece, November 2000.
- Steven M. Bellovin, Adam Buchsbaum, and S. Muthukrishnan. TCP compression filter. Obsolete Internet draft, October 1999.
- Steven M. Bellovin, Adam Buchsbaum, and S. Muthukrishnan. TCP filters. Obsolete Internet draft, October 1999.
- Steven M. Bellovin. Distributed firewalls. *;login:*, pages 39–47, November 1999.
- J. S. Denker, S. M. Bellovin, H. Daniel, N. L. Mintz, T. Killian, and M. A. Plotnick. Moat: A virtual private network appliance and services platform. In *Proceedings of LISA XIII*, November 1999.
- Peter Gregory. Why systems administration is hard. In *Solaris Security*. Prentice-Hall, 1999. (Foreword).
- Fred Schneider, Steven M. Bellovin, and Alan Inouye. Critical infrastructures you can trust: Where telecommunications fits. In *Telecommunications Policy Research Conference*, October 1998.
- William Cheswick and Steven M. Bellovin. How computer security works: Firewalls. *Scientific American*, pages 106–107, October 1998.
- Steven M. Bellovin. Cryptography and the Internet. In *Advances in Cryptology: Proceedings of CRYPTO '98*, August 1998.
- S. Bellovin. Report of the IAB Security Architecture Workshop. RFC 2316, RFC Editor, April 1998.
- H. Lu, M. Krishnaswamy, L. Conroy, S. Bellovin, F. Burg, A. DeSimone, K. Tewani, P. Davidson, H. Schulzrinne, and K. Vishwanathan. Toward the PSTN/Internet Inter-Networking–Pre-PINT Implementations. RFC 2458, RFC Editor, November 1998.

- Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, and Bruce Schneier. The risks of key recovery, key escrow, and trusted third-party encryption, May 1997. A report by an ad hoc group of cryptographers and computer scientists.
- Yakov Rekhter, Paul Resnick, and Steven M. Bellovin. Financial incentives for route aggregation and efficient address utilization in the Internet. In *Proceedings of Telecommunications Policy Research Conference*, 1997.
- Steven M. Bellovin. Probable plaintext cryptanalysis of the IP security protocols. In *Proc. of the Symposium on Network and Distributed System Security*, pages 155–160, 1997.
- Bill Cheswick and Steven M. Bellovin. A DNS filter and switch for packet-filtering gateways. In *Proceedings of the Sixth Usenix Unix Security Symposium*, pages 15–19, San Jose, CA, 1996.
- Steven M. Bellovin. Problem areas for the IP security protocols. In *Proceedings of the Sixth Usenix Unix Security Symposium*, pages 205–214, July 1996.
- David A. Wagner and Steven M. Bellovin. A "bump in the stack" encryptor for MS-DOS systems. In *Proceedings of the Symposium on Network and Distributed System Security*, pages 155–160, San Diego, February 1996.
- Uri Blumenthal and Steven M. Bellovin. A better key schedule for DES-like ciphers. In *Proceedings of PRAGOCRYPT '96*, Prague, 1996.
- S. Bellovin. Defending Against Sequence Number Attacks. RFC 1948, RFC Editor, May 1996.
- Steven M. Bellovin. Using the domain name system for system break-ins. In *Proceedings of the Fifth Usenix Unix Security Symposium*, pages 199–208, Salt Lake City, UT, June 1995.
- Steven M. Bellovin. Security and uses of the Internet. In *Proceedings of the North American Serials Interest Group*, June 1995.
- Matt Blaze and Steven M. Bellovin. Session-layer encryption. In *Proc. 5th USENIX UNIX Security Symposium*, Salt Lake City, UT, June 1995.
- David A. Wagner and Steven M. Bellovin. A programmable plaintext recognizer, 1994. Unpublished.
- S.M. Bellovin and W.R. Cheswick. Network firewalls. *IEEE Communications Magazine*, 32(9):50–57, Sept 1994.
- Steven M. Bellovin and Michael Merritt. An attack on the *Interlock Protocol* when used for authentication. *IEEE Transactions on Information Theory*, 40(1):273–275, January 1994.

- S. Bellovin. Firewall-Friendly FTP. RFC 1579, RFC Editor, February 1994.
- S. Bellovin. Security Concerns for IPng. RFC 1675, RFC Editor, August 1994.
- S. Bellovin. On Many Addresses per Host. RFC 1681, RFC Editor, August 1994.
- Steven M. Bellovin and Michael Merritt. Augmented encrypted key exchange. In *Proceedings of the First ACM Conference on Computer and Communications Security*, pages 244–250, Fairfax, VA, November 1993.
- Steven M. Bellovin. Packets found on an internet. *Computer Communication Review*, 23(3):26–31, July 1993.
- Steven M. Bellovin. A best-case network performance model, 1992. Unpublished.
- Steven M. Bellovin. There be dragons. In *Proceedings of the Third Usenix Unix Security Symposium*, pages 1–16, September 1992.
- Steven M. Bellovin and Michael Merritt. Encrypted key exchange: Password-based protocols secure against dictionary attacks. In *Proc. IEEE Computer Society Symposium on Research in Security and Privacy*, pages 72–84, Oakland, CA, May 1992.
- Steven M. Bellovin and Michael Merritt. Encrypted key exchange: Password-based protocols secure against dictionary attacks, August 1991.
- Steven M. Bellovin and Michael Merritt. Limitations of the Kerberos authentication system. In *USENIX Conference Proceedings*, pages 253–267, Dallas, TX, Winter 1991.
- Steven M. Bellovin, November 1990. Internal report.
- Steven M. Bellovin and Michael Merritt. Limitations of the Kerberos authentication system. *Computer Communication Review*, 20(5), October 1990.
- Steven M. Bellovin. Pseudo-network drivers and virtual networks. In *USENIX Conference Proceedings*, pages 229–244, Washington, D.C., January 1990.
- Steven M. Bellovin. Towards a commercial IP security option. In *Commercial IPSO Workshop, INTEROP '89*, 1989.
- Steven M. Bellovin. Security problems in the TCP/IP protocol suite. *Computer Communication Review*, 19(2):32–48, April 1989.
- Steven M. Bellovin. The "session tty" manager. In *Proc. Usenix Conference*, Summer 1988.
- Peter Honeyman and Steven M. Bellovin. PATHALIAS or the care and feeding of relative addresses. In *Proc. Summer Usenix Conference*, 1986.

Major Positions

2013–2015 Member, National Research Council study committee on FAA Next Generation Air Traffic Control System

2012–now Member, National Research Council study committee on Cybersecurity Foundations

2010–now Member, Computer Science and Telecommunications Board of the National Academies

2009–2012 Member, Technical Guidelines Development Committee of the Elections Assistance Commission

2008 Co-chair, Applied Cryptography and Network Security (ACNS)

2006 Chair, Steps Towards Reducing Unwanted Traffic in the Internet (SRUTI)

2005–now Member, Department of Homeland Security Science and Technology Advisory Committee

2004–2007 Member, National Research Council study committee on cybersecurity research needs.

2002–2004 Member, ICANN DNS Security and Stability Advisory Committee.

2002–2004 Security Area co-director, Internet Engineering Task Force (IETF).

2002 Chair, program committee, IEEE Symposium on Security and Privacy.

2002 Member, Information Technology sub-committee, National Research Council study committee on science and technology against terrorism.

2001–2003 Member, ACM Advisory Committee on Security and Privacy.

2001 Vice-chair, program committee, IEEE Symposium on Security and Privacy.

2001–2003 Member, National Research Council study committee on authentication technologies and their privacy implications.

2000–2002 Chair, IETF ITRACE working group.

2000 Co-chair, Usenix Security Symposium.

1999–2002 IETF representative, ICANN Protocol Supporting Organization

1999–now Co-chair, IETF SPIRITS working group.

1997–2001 Co-chair, IETF PINT working group.

1996–1998 Member, National Research Council study committee on information systems trustworthiness.

1996–2002 Member, Internet Architecture Board.

1996 Co-chair, Usenix Security Symposium.

1993–1995 Member, IETF IPng Directorate.

U.S. Patents

8,798,614 Enhanced communication service for predicting and handling communication interruption

8,676,916 Method and Apparatus for Connection to Virtual Private Networks for Secure Transactions

8,239,531 Method and Apparatus for Connection to Virtual Private Networks for Secure Transactions

8,145,793 System and Method for Distributed Content Transformation

8,107,479 Method and System for Telephony and High Speed Data Access on a Broadband Access Network

8,037,167 Method for Detecting Hosts behind Network Address Translators

7,907,517 Routing Protocols with Predicted Outage Notification

7,756,008 Routing Protocols with Predicted Outage Notification

7,676,224 Enhanced Communication Service for Predicting and Handling Communication Interruption (2010).

7,558,970 Full-Text Privacy-enhanced searches using encryption

7,227,843 Method for reducing congestion in packet-switched networks (2007).

7,051,365 Method and apparatus for a distributed firewall (2006).

7,035,410 Method and apparatus for enhanced security in a broadband telephony network (2006).

6,870,845 Method for providing privacy by network address translation (2005).

6,665,299 Method and system for telephony and high speed data access on a broadband access network (2003).

5,958,052 Method and apparatus for restricting access to private information in domain name systems by filtering information (1999).

5,870,557 Method for determining and reporting a level of network activity on a communications network using a routing analyzer and advisor (1999).

5,805,820 Method and apparatus for restricting access to private information in domain name systems by redirecting query requests (1998).

5,440,635 Cryptographic protocol for remote authentication (1995).

5,241,599 Cryptographic protocol for secure communications (1993).

Numerous other patent applications are pending.